How the State Declarations Portal Provides A Secure Communication Channel with the Department of Safeguards

John Murray, Michelle Mock, Paul Kaiser, and Evan Crawford

International Atomic Energy Agency
Vienna International Centre, PO Box 100
A-1400 Vienna, Austria
Email: j.murray@iaea.org, m.mock@iaea.org, paul.kaiser@iaea.org, e.crawford@iaea.org

Abstract

This paper will demonstrate the features and benefits of the State Declarations Portal (SDP). Historically, there have been many channels of communication, including traditional mail, fax, email, and other custom secure channels. This presented a wide array of options when sending and receiving information. The SDP was developed to provide external users a single, preferred channel to communicate with the Department of Safeguards in a secure manner. The SDP is a modern, web-based, application that may be accessed from any Internet-connected computer. It allows timely and secure communications despite worldwide Covid-19 related lockdowns, where traditional mail may be unreliable and many people are working from home. The SDP is secured with a multi-layered approach, including the use of two-factor authentication and asymmetric encryption. Within a State or regional authority, other actors, such as Facility Operators, may also participate in this channel in a siloed manner. Other features include the ability to add non-formal comments related to communications. Finally, the SDP aids in long-term knowledge management. The records of all incoming and outgoing communications, including comments, are available to active users in the Portal. Users are able to filter and search for particular records. This establishes a shared history with the Department of Safeguards and ensures continuity of knowledge over time.

Keywords: SDP, State Declarations Portal, safeguards, encryption, two-factor authentication, knowledge management

Introduction

In 2020 alone, the International Atomic Energy Agency (IAEA) received, processed, and registered 23,682 official communications in various forms from Member States. This number does not include the number of unofficial communication transactions that are ongoing daily at the working level. As communication and information exchange between Member States and the IAEA has increased over time, the need for a single channel that moved away from traditional forms of communication (e.g. facsimile, letters, email, etc.) and that supported secure, prompt, and timely information exchange has also increased. The State Declarations Portal (SDP) was designed and launched to support the exchange of information and communication between Member States and the IAEA Department of Safeguards.

This paper summarizes the history, challenges, and usage of the SDP, and details the multi-layered security approach implemented therein. The SDP has improved the effectiveness, efficiency, and security of information exchange between Member States and the Department of Safeguards. This paper focuses on the current state of the SDP; additional features are planned to provide a more secure, improved user experience for Member States, but are outside the scope of this paper.

A History of Communications with Safeguards

> *Each Member should make available such information as would, in the judgement of the member, be helpful to the Agency.*
>
> *IAEA Statute - Article VIII Section A*

Upon its creation in 1957, the IAEA was tasked with the mission to "promote and control the Atom" (International Atomic Energy Agency, n.d.-a). This role entailed engaging in numerous activities, one of which was to receive information from and correspond with Member States regarding nuclear activity. In the beginning, information gathering and correspondence by the IAEA was processed and evaluated manually. However, it soon became evident that manual processing would not be feasible nor sustainable for the future. Information systems, like that of the IAEA's Safeguards Information System (ISIS), were developed in 1977 (International Atomic Energy Agency; 1984, October) and communication systems, like that of the Safeguards Documents Unit which was established in 1983, were created to receive, manage, and disperse the ever-increasing flow of nuclear safeguards information and correspondence.

Information sent by Member States was received in a variety of ways and in a variety of formats. In the beginning, most States sent correspondence and information by post or by hand delivery. The first submission that involved a transfer of material with sampling was received by the Department of Safeguards via post in 1959. Nearly 40 years later, in March of 1998, the first Additional Protocol declaration received was also sent by post. However, with the slow and steady advancement of communication and information technology, the receptacles for information became more varied. States would share and exchange information and data in meetings, on mini-data microfilms, cassettes, JAZ disks, ZIP disks, CD-ROMs, letters, facsimile, USB sticks, and, more frequently today, email. The overall goal seemingly to get closer to more efficient, effective, and secure communication and information exchange.

Communication Challenges

As evidenced by the aforementioned history of communicating with Safeguards, striving towards efficient, effective, and secure communication and information exchange with Member States on nuclear safeguards has been an ongoing and evolving process. Over the many decades, this evolving process has been challenging and has often hampered the end goal of streamlining the ability of Member States to communicate with the Department of Safeguards and vice versa.

Due to the numerous channels of communication (e.g. letters, facsimile, USB sticks, emails, and bespoke secure systems like that of the Safeguards Mailbox) communicating with the Department of Safeguards was not straightforward. The lack of clarity posed questions, such as: how did one know which channel to use to ensure that the piece of information would be received by and sent to the intended recipient; if the information being conveyed was time sensitive, which method was the fastest method of communication? Easy answers to these questions were unclear despite previous efforts made to communicate which channel should be used for what purpose.

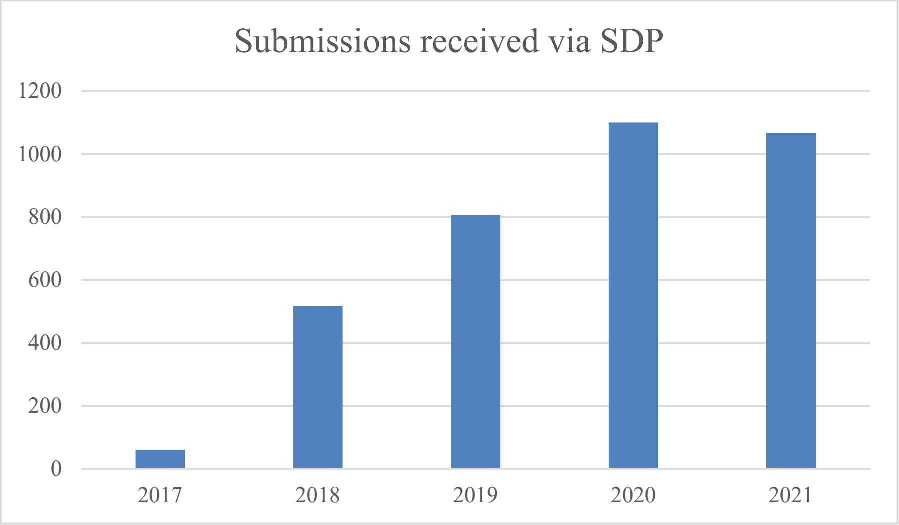
The workflow for many of these traditional communication and information systems involved multiple individuals, various handoff points, numerous transition stages, and potential delays in the transfer of information or communication. Few of the numerous channels of communication supported a streamlined workflow in which the information sent was directly received by the receiver with few individuals being involved, no handoffs needed, no various transition points, or a decrease in the time to transfer or convey the information to the end receiver.

As email became a widely accepted form of communication it became the *de facto* answer to both Member States' and the Department of Safeguards' need for efficient and direct communication and information exchange on nuclear safeguards. However, even this answer allows room for inefficiency and disorganization: there are now numerous email addresses to keep track of and one must recall what information goes to which address; workflow knowledge and knowledge retention is challenging when an email inbox is shut down upon an individual leaving, either on the side of the Member State or the Department of Safeguards; and there are various security risks associated with email.

The SDP was created not only to have a secure method for sending and receiving information with the Department of Safeguards at the IAEA, but also to be a single channel for all communication and information exchange on the topic of nuclear safeguards. The principal achievement of the SDP is that virtually any information and file type can be sent via the SDP and can be directly received by the intended recipient at the Department of Safeguards. Furthermore, the SDP's use of a multi-layered security approach assures a high level of security and confidentiality. Additionally, the SDP provides an easily-accessible historical record of communication between Member States and the Department of Safeguards.

The State Declarations Portal (SDP) in Use

Since its launch in May of 2017, use of the SDP has steadily grown and is now used by 94 Member States. By the end of the first half of 2021, the SDP had ***284*** active Member State users, the Department of Safeguards had received ***3551*** submissions from Member States via the SDP, and the Department had sent out ***678*** reports to Member States via the SDP. The following graph shows the submissions received since 2017. The figures demonstrate a steady increase in the usage of the SDP, which is expected to continue.



Graph 1. Total submissions received from Member States via the SDP from May 2017 through July 2021.

These figures demonstrate that the SDP has initiated a shift in communication and information exchange from other more traditional communication channels available to Member States (e.g. hard copy, storage devices, email).

Due to its efficiency, effectiveness, and security, the SDP has become routinely used as a communication and information exchange resource within the Department of Safeguards for the rapid exchange of sensitive and confidential information with Member States.

Security Overview

In *An Introduction to Information Security*, the National Institute of Standards and Technology (NIST) defines information security as

> *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability. (Nieles, M., Dempsey, K., & Pillitteri, V. Y., 2017).*

This introduces three key aspects that NIST defines as:

- **Confidentiality** – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity** – Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
- **Availability** – Ensuring timely and reliable access to and use of information.

Multiple measures have been implemented in the SDP to protect the confidentiality, integrity, and availability of the information that is exchanged via the SDP.

Security risks can occur at a variety of levels; therefore, security measures must provide multiple layers of defence. In fact, a fundamental design principle is layering. “Layering refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems” (Stallings, W., & Brown, L., 2015). Layering is also referred to as defence in depth. The main layers to consider are system, network, application, and transmission.

System level security consists of hardening the operating system(s) and putting the proper controls for access in place. Network level security assures against unauthorized access and intrusion. Here, for example, firewalls may be considered an integral component of network level security. As system and network level security describe measures that pertain to sensitive internal systems at the IAEA, this paper will not describe them in detail but rather focuses on the application and transmission layers. Of course, maintaining a secure infrastructure is an ongoing process. In 2018, “…strengthened information security” (International Atomic Energy Agency, 2018 December) was a key component of the completed Modernization of Safeguards Information Technology (MOSAIC) project. This included creating a “Single integrated & secure environment for all safeguards information” (International Atomic Energy Agency, n.d.-b).

The SDP is a web-based application – it is essentially a website that users outside of the IAEA may access. As a publicly accessible website, it is vital that the application is secure. Various technologies have been implemented to provide security at the Application and Transmission layers.

Secure Sockets Layer (SSL)

The very first layer of security that a user will encounter is the Hypertext Transfer Protocol Secure (HTTPS), or Hypertext Transfer Protocol (HTTP) over Secure Sockets Layer (SSL). SSL is “a protocol used for protecting private information during transmission via the Internet” (National Institute of Standards and Technology, n.d.). HTTPS contributes to two aspects of security: integrity and confidentiality. HTTPS provides integrity by ensuring the user has reached the authentic SDP site. All modern browsers support HTTPS and will warn the user if the connection is not secure. The user can also view the digital certificate – this ensures the authenticity of the provider of the web site (for the SDP, it is the International Atomic Energy Agency) – “the website's server uses a certificate to prove the website's identity to browsers” (Google, n.d.). For confidentiality, the data exchanged over HTTPS is encrypted.

Authentication

The next layer of security is access. Access to the SDP is restricted, working on a zero-trust model where all users are effectively untrusted (Kindervag, J.; 2010, October 6). The SDP relies on multi-factor authentication (MFA) to confirm the identity of external users. Multi-factor authentication is the use of multiple factors to confirm the identity of someone who is requesting access to the SDP. “By requiring people to confirm identity in more than one-way, multi-factor authentication provides greater assurance that they really are who they claim to be—which reduces the risk of unauthorized access to sensitive data” (SecurID., 2021, June 28).

The SDP utilizes the following factors for identification:

1. **Something you know** – a personal identification number (PIN)
2. **Something you have** – a hardware token that generates a one-time password (OTP)

All users of the SDP are assigned a piece of hardware known as an RSA SecurID token. The token generates a new OTP every sixty seconds. As soon as the OTP is entered, it is no longer valid. When performing a login to the SDP, the user combines their PIN with the OTP generated by the token.

Strong authentication ensures confidentiality through strictly controlling the access to information. It also maintains integrity by ensuring the authenticity of the user accessing the SDP.

Information Security

Information that is exchanged with Member States takes two forms: files and metadata. The Safeguards relevant information – either structured data (such as Nuclear Material Accounting Reports) or textual documents – is contained within submitted files. Metadata exchanged includes the Member State name, submitting user’s identity, date, and description.

The submitted file is transmitted from the user’s computer, over the Internet to the externally facing SDP, then through the IAEA’s internal network, and finally to the Safeguard’s secure network. Throughout this process the submitted files will be both stored on, and transmitted between, multiple servers.

> *State policy on the security of information should define which type of information the State wishes to be secured and indicate how that security is to be applied. (International Atomic Energy Agency, 2015)*

Information submitted to the Department of Safeguards has to be protected according to its ascribed classification level. The responsibility for defining the level of information security of a submission to the Department of Safeguards rests with the Member State making the submission. To simplify the information handling process – as well as to mitigate potential classification errors – the SDP simply requires that all submitted files are encrypted. The files are then decrypted only within the Department of Safeguards’ internal safeguards network, allowing for existing confidential data handling processes within the Department of Safeguards to be maintained.

Encryption

To protect the files throughout the journey from the computer at the Member State to the secure network at the Department of Safeguards, it was decided that all files would be encrypted. "One of the most effective methods for protecting … data is via encryption" (RSI Security, 2019). The files remain encrypted "end-to-end" – both in transmission and at rest. Encryption ensures against unauthorized access (confidentiality), as well as protects against information modification and maintains authenticity (integrity).

To put it simply, encryption allows data to be accessed and decrypted only by someone with the correct key (RSI Security, 2019). There are two types of encryption: symmetric and asymmetric. The SDP uses Public Key cryptography, which uses asymmetric encryption.

> *Public key encryption allows each person in a conversation to create a public key and a private key. The two keys are connected and comprised of extremely large numbers with complex mathematical properties. This makes it so that data that one person encrypted using their public key can only be decoded by another when using their matching private key. (RSI Security, 2019)*

The Member State user encrypts the files using the IAEA Public Key; therefore, only the IAEA is able to decrypt these files. The user must encrypt all files prior to uploading them via the SDP. The SDP application enforces this rule to ensure the user does not submit unencrypted files by mistake. Once the encrypted files are uploaded, they are attached to a "Submission", which is then transmitted via the SDP to the IAEA. The files received from the Member State are only decrypted within the IAEA's secure network.

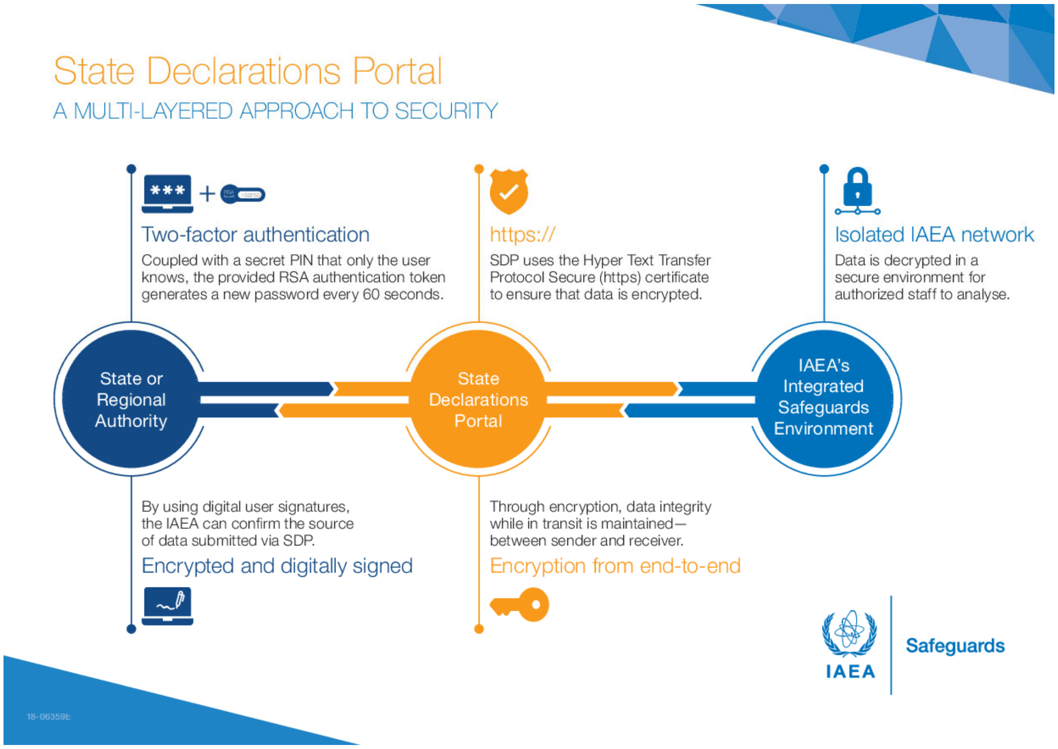
When the IAEA wants to send, or "publish", files via the SDP to the Member State, one or more files are combined together into a "Report Package" file. This Report Package is then encrypted for one or more users from the Member State. Each user from a Member State must provide a Public Key to the IAEA upon registering for the SDP, which is used to encrypt all files sent to that user. The IAEA can encrypt for one, some, or all of the users from a Member State.

Digital Signatures

Public key cryptography can also be used for authentication, which ensures the authenticity of files transmitted via the SDP. The files must also be digitally signed with the user's Private Key. The digital signature can then be verified using the Public Key of the person or entity that created the signature. The digital signature ensures the integrity of the transmitted files. "A valid digital signature gives the recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit" (Groom, Groom, & Jones, 2017).

The IAEA verifies the signature of all files received via the SDP after decryption, which provides additional assurances that the file is indeed from the Member State user and that the file has not been tampered with during transmission. Likewise, all Report Packages that the IAEA publishes to the Member State are also digitally signed with the IAEA Private Key, which provides further trust to the Member State user that the information has come from the IAEA and has not been tampered with during transmission.

The various technologies and layers used to the secure the information exchanged via the SDP are summarised in the infographic below.



State Declarations Portal

A MULTI-LAYERED APPROACH TO SECURITY

Two-factor authentication

Coupled with a secret PIN that only the user knows, the provided RSA authentication token generates a new password every 60 seconds.

https://

SDP uses the Hyper Text Transfer Protocol Secure (https) certificate to ensure that data is encrypted.

Isolated IAEA network

Data is decrypted in a secure environment for authorized staff to analyse.

***
State or Regional Authority
State Declarations Portal
IAEA's Integrated Safeguards Environment
IAEA
Safeguards
18-06359E

By using digital user signatures, the IAEA can confirm the source of data submitted via SDP.

Encrypted and digitally signed

Through encryption, data integrity while in transit is maintained—between sender and receiver.

Encryption from end-to-end

Safeguards Relevance

When, pursuant to a safeguards agreement, a Member State declares nuclear materials, submits quarterly and annual declarations, or corresponds with the Department of Safeguards, the State must decide which channels are appropriate. The selected channel must ensure that the intended recipient receives the submission in a timely manner, with assurances that risks to confidentiality or tampering have been minimized.

Web-based applications which are accessible to only authorized users, such as the SDP, can mitigate these risks. The SDP leverages information technology by maintaining the history of all submissions and communications between Member States and the Department of Safeguards, thereby increasing the effectiveness of safeguards. The SDP improves the efficiency and effectiveness of safeguards by offering a direct one-to-one communication channel. Currently the SDP provides the most secure communication channel between Member States and the Department of Safeguards due to the SDP's multi-layered security approach.

The SDP's core features and functionalities improve the effectiveness, efficiency, and security of correspondence between Member States and the Department of Safeguards. The historical record of all communication allows for knowledge retention by both the Member State and the Department of Safeguards. This feature captures the knowledge of the individual working within the organization, aiding in knowledge retention and transparency of workflows, benefitting not only the IAEA, but the Member States as well.

Conclusion

According to the current Director of the Department of Safeguards' Division of Information Management, "Information is at the heart of modern nuclear verification" (Baute, J., 2006). From its inception, and as articulated in its Statute, the IAEA has relied on the exchange of information with its Member States to fulfil its mission. As the exchange of information is critical for nuclear verification, it is essential to make the exchange efficient, effective, and secure. The SDP was developed and launched to meet those challenges.

In the future, the SDP will continue to integrate additional features, benefits, security features, and more user-friendly interfaces to ensure that the SDP remains the most efficient, effective, and secure method of communication between the Department of Safeguards and Member States. As a web-based application, the SDP provides a convenient communication and information system that ensures a bright future for communications between Member States and the Department of Safeguards

Acknowledgements

We thank the IAEA Archives and Records Management Section for their exceptional support and expertise in providing background information and data for this paper.

References

Baute, J. (2006). Safeguards information challenges. ADDRESSING VERIFICATION CHALLENGES, 51–56. https://www.pub.iaea.org/MTCD/publications/PDF/P1298/P1298_Contributed_Papers.pdf

Google. (n.d.). Check if a site's connection is secure. Google Chrome Help. Retrieved July 22, 2021, from https://support.google.com/chrome/answer/95617?hl=en#zippy=%2Csecure

International Atomic Energy Agency. (n.d.-a). History. Retrieved July 22, 2021, from https://www.iaea.org/about/overview/history

International Atomic Energy Agency. (n.d.-b). MOSAIC: Modernization of Safeguards IT [Infographic]. https://www.iaea.org/sites/default/files/16/09/mosaic_infographic.pdf

International Atomic Energy Agency. (1984, October). IAEA Safeguards Information System (ISIS) (IAEA-TECDOC-316). INIS Clearinghouse. https://inis.iaea.org/collection/NCLCollectionStore/_Public/16/022/16022428.pdf?r=1&r=1

International Atomic Energy Agency. (2018, December). Nuclear Verification 1,2. IAEA Annual Report 2018. https://www.iaea.org/sites/default/files/publications/reports/2018/gc63-5-nuclear-verification.pdf

Jones, S. S., Groom, K. M., & Groom, K. (2017). Network and Data Security for Non-Engineers. CRC Press.

Kindervag, J. (2010, October 6). WEBINAR: Zero Trust Network Architecture [Video]. Forrester. https://www.forrester.com/webinar/Zero+Trust+Network+Architecture/-/E-WEB6792#

National Institute of Standards and Technology. (n.d.). Secure Sockets Layer (SSL). Computer Security Resource Center. Retrieved July 22, 2021, from https://csrc.nist.gov/glossary/term/secure_sockets_layer

New Web-Based System Streamlines Safeguards Information Exchange With IAEA. (n.d.). Retrieved from IAEA.org: https://www.iaea.org/newscenter/news/new-web-based-system-streamlines-safeguards-information-exchange-with-iaea

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security. National Institute of Standards and Technology, 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Scott Rose, O. B. (n.d.). Zero Trust Architecture. Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

SecurID. (2021, June 28). What is Multi-Factor Authentication (MFA) – RSA. SecurID.Com. https://www.securid.com/en-us/blog/the-language-of-cybersecurity/what-is-mfa

Stallings, W., & Brown, L. (2017). Computer Security: Principles and Practice (4th ed.).